Remarks/Arguments

Applicants appreciate the courtesy shown to their attorney during telephone interviews with the Examiner and the Examiner' supervisor, Glenton Burgess, concerning the effective date of the primary cited reference, as discussed below.

Claims 11 and 12, which were rejected, 35 USC 112, second paragraph, have been amended as suggested by the Examiner. Withdrawal of the Section 112 rejection is therefore requested.

Claims 3, 4, 9, 10, 11, and 12 have been amended to improve their form.

Claims 5 and 6 were indicated by the Examiner as being allowable if rewritten in independent form including all of the limitations of their base and intervening claims. These claims have been thus amended and their reconsideration and allowance are therefore requested.

Claims 1-2, 7-10, 13-16, and 18-21 were rejected, 35 USC 102(e), as anticipated by Copeland Patent Application Publication 2002/0244156. Claim 3 was rejected, 35 USC 103(a), as being unpatentable over Copeland in view of Kaku patent 6,279,097, and claim 4 as being unpatentable over Copeland and Kaku further in view of Satoh et al patent 6,065,064. Accordingly, the primary reference is the Copeland published application, which has a filing date of January 31, 2002.

Applicants note that their application has a filing date July 20, 2001 which is prior to the Copeland application filing date. Accordingly, while the Examiner has at great length analyzed and applied the Copeland patent publication disclosure to applicants' claims, that disclosure is not itself available as a reference against applicants' claims. Instead one must look at the disclosure set forth in the Copeland provisional application 60/265,194, filed Jan. 31, 2001. Applicants have obtained a copy of this provisional application, and a copy thereof is enclosed for the Examiner's review and consideration.

Unlike the Published Patent Application, the provisional application is a very short (four pages) discussion of network vulnerabilities and appears to focus on what Copeland refers to as LAN scope as a way to detect possible network attacks. It contains no drawings and no detailed discussion of the technology involved. It is certainly not an enabling disclosure to support the non-provisional Copeland application.

Applicants submit that the teaching and disclosure of this Provisional Application does not contain the specific disclosure relied upon by the Examiner in the Office Action and that therefore the Copeland disclosure in the non-provisional patent application is not available as prior art against applicants' invention.

Applicants also wish to point out to the Examiner that the Copeland Provisional Application itself is neither a disclosure or a teaching of applicants' invention. Copeland is directed to an entirely different problem than applicants' invention. In Copeland the goal and result are to identify flows and analyze abnormal behavior for intrusion detection. As such, Copeland requires identification of port numbers and mapping of those port numbers to applications (Web, FTP...). In fact, as clearly seen in the Copeland abstract, Copeland describes his invention as "A port profiling system detects unauthorized network usage."

Applicants' goal is to identify flows that are characterized by source and destination addresses only and specifically does not involve processing of port information or port addresses. Applicants address problems of monitoring a network to assure that network performance is such as to provide a high quality of service to customers. Further applicants enable the identification of IP flows between two monitoring points so that the configuration of the monitors can be automated. Thus, the applications, the actual meaning of "flows", and the mechanisms and steps for identifying the flows in Copeland and in applicants' invention are all different.

Accordingly, applicants request withdrawal of the Copeland Published Patent Application as prior art and reconsideration and allowance of claims 1-4 and 7-21, in addition to claims 5 and 6, and passage of this application to issue.

If the Examiner considers it would in any way expedite the prosecution of this application, the Examiner is invited to telephone applicants' attorney at the number set forth below.

Respectfully submitted,

C. L. Lau et al

By____________________
James W. Falk
Attorney for Applicants
Reg. No. 16,154
(732) 699-4465

Enclosed:
Provisional Application 60/265,194

02 01 01 AIPREV

Please type a plus sign (+) inside this box ⟶ ⊞

PTO/SB/16 (8-00)
Approved for use through10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
John A.	Copeland, III	1070 Greenway, Atlanta, GA 30350

□ Additional inventors are being named on the ___ separately numbered sheets attached hereto

TITLE OF THE INVENTION (280 characters max)

The Use of "Flows" to Analyze Data Network Traffic

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ Customer Number 24728 ⟶

24728
PATENT TRADEMARK OFFICE

OR

Type Customer Number here

□ Firm or Individual Name	John T. Winburn				
Address					
Address					
City		State		ZIP	
Country		Telephone	404-233-7000	Fax	

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages	4	□ CD(s), Number	
□ Drawing(s) Number of Sheets		☒ Other (specify)	Petition for Prov. App.
□ Application Data Sheet. See 37 CFR 1.76			

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.

☒ A check or money order is enclosed to cover the filing fees

□ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: ______

□ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) $75

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

□ Yes, the name of the U.S. Government agency and the Government contract number are: ______

Respectfully submitted,

SIGNATURE JW

Date 01-31-01

TYPED or PRINTED NAME John T. Winburn

REGISTRATION NO. (if appropriate) 26,822

Docket Number: 10775-33182

TELEPHONE 404-233-7000

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

The Use of "Flows" to Analyze Data Network Traffic

by Dr. John A. Copeland
Draft Jan. 2, 2001

Suppose you are responsible for a corporate network. The company is improving productivity by continually running additional network enabled applications over this network. While the network opens windows to the world, open windows can be used by outsiders to exploit vulnerabilities. What are the possibilities that you want to guard against.

Threats

One primary danger to avoid is having outside hackers getting control of a computer (host) on your network. Once "in," they can download private company data, use the host to attack other hosts from inside the firewall, or use the host to scan and attack other computers anywhere in the world, with your network getting the initial blame. Such a takeover from the outside involves three stages:

> Stage 1. a scan of your network to determine what type of computers are on your network, their operating systems, their network listener applications (servers), and their Internet Protocol addresses and open port numbers,
>
> Stage 2. application of an exploit routine that allows the attacker to gain access to the computer, and
>
> Stage 3. the operation of an application that accomplishes the attacker's objectives.

Another technique being seen with increasing frequency is the installation of a Trojan Horse program by an innocent looking program, such as an email or network news attachment. In this case stage 3 is the first stage that shows up in network activity.

If you know what activities are normal for your network in great enough detail, stages 1 and 3, and sometimes stage 2, are detectable as "abnormal" network activities (what LANcope calls "Out of Profile" activities). The exploit routine in stage 2 can be detected by a signature-based Intrusion Detection System (IDS), but only if it has been seen before, captured, and analyzed by the IDS vendor.

Characterizing and Tracking Network Activities

In order to provide knowledge about what is transpiring over an Internet Protocol (IP) data communications network, we need to partition the packets into groups that represent a complete communication transaction between two hosts (computers). There are dozens of Transport Layer protocols that can be running on an IP network. Most host-to-host communications will be carried by the Transport Control Protocol (TCP). TCP establishes "connections" that carry a stream of data in multiple packets. These packets are numbered so that they can be assembled, by the receiving host, in the correct order with no gaps (missing packets are retransmitted by the source host). Many times hosts will use multiple simultaneous and/or sequential TCP connections to carry out a communications session.

The User Datagram Protocol (UDP) is another Transport Layer Protocol that is carried by IP networks. This was originally designed for sending quick single-packet messages, such as a host asking a Domain Name Server for the IP numeric address associated with a URL, like www.LANcope.com. Today it is also being used to carry streams of multimedia content where reliable delivery and packet acknowledgement is not needed.

The LANcope Monitor program looks at each packet and assigns it to a "Flow." A Flow is defined, in this case, as the packets exchanged between two hosts that are associated with a single "service." Examples of a service would be using a Web browser to access a single Web server, or using an email program to access a mail server. With UDP, an example of a Flow would be the stream of packets that carry data from a Multimedia server to a host with the appropriate "player" (e.g., a Web Radio client).

Most Intrusion Detection Systems piece together the packets in a TCP connection to collect the stream of bytes being transmitted, and then look for certain strings of characters in the data (signatures). These signatures are particular text strings that have been discovered in known hacker "exploits." The more signatures in the IDS's collection, the longer it takes to do an exhaustive search on each data stream. Even with all this effort, this technique will not recognize a brand new exploit that has not been analyzed to find a signature.

After LANcope associates each packet with a Flow, certain statistical data is updated in the Flow data record (number of bytes, packets, flag-bit combinations, etc.). No string search is made for signatures. This technique also is used for UDP Flows. When the Flow ends, the statistical data is examined to determine the type of transaction that took place, and the data records on the hosts involved is updated to reflect the new Flow information.

Analyzing data at the flow level has several advantages. By collecting data on the complete transaction (the Flow) before analysis, better decisions can be made. For example host Trudy sends three packets to host Bob with a source port number fixed at 64,000 and destination port numbers of 21, 25, and 111. Treated as one Flow, this is quickly determined to be a port scan since the source port number did not vary.

Without this step, the probe above would lead to the erroneous conclusion that host Bob was running server programs on ports 23, 25, and 111 (Telnet, SMTP, and SunRPC). Since Bob responded with TCP Reset packets he should not be credited with operating these server applications.

If the data were collected as three different TCP connections, each connection could be due to a common type of error seen on networks. A further correlation step for all TCP connections would be necessary before the important conclusion, made quickly from the a single Flow data record, could be made. Since there can be many simultaneous TCP connections in progress or recently ended, a good bit of CPU time would be required to continually search for such a correlation.

Recently a typical network had an average of 5 TCP or UDP connections per Flow, 160 packets per Flow, and 50,000 bytes per Flow. While the numbers vary from network to network and day to day, the number of data records to analyze are much smaller when collected on a Flow basis.

The analysis of data by Flow allows LANcope to distinguish normal connections, usually between a client and server, from incomplete or rejected transactions (potential probes). A misleading picture of network activity would result if the probes generated by a hacker for scanning or exploitation, or even common connection errors, were treated as actual network connections.

LANcope examines each flow to see if it has characteristics of a possible probe used by a hacker to map out the network, possibly looking for hosts vulnerable to various exploits or attacks. These probes sometimes are unnatural, and give themselves away immediately. Other times they resemble erroneous or unsuccessful connections that are seen frequently due to normal network operations, and only by correlation with other events can be recognized as part of a scanning or probing activity. To correlate these events, each time a host is responsible for a potential probe, its Concern Index is increased by a certain amount.

By analogy, if a stranger rattled your front door and then said he had the wrong address, you would have no basis to call the police. If he continued down the street doing the same thing, his Concern Index would increase to the point the calling the police would be appropriate (an IP address scan). The same would be true if he rattled other doors in the same house (a TCP or UDP port scan)

LANcope also examines each Flow shortly after it starts to see if is an Attack, such as a Half-Open Denial of Service Attack, so that immediate notification to network managers can be made.

Exploitation Detection

As anyone who has connected a PC to a cable modem and run a program like Black Ice or Zone Alert knows, any given IP address is likely to be scanned a dozen times a week. These scans come from various countries around the world, perhaps from hosts that have previously been compromised. After a while, one upgrades his operating system to the latest (security-fix) releases, closes ports that do not need to be open, and ignores the scans that are looking for vulnerable systems (however, today's secure system may be tomorrow's vulnerable system). LANcope notes these scans, and provides data on the scanning host that can be obtained from techniques such as a DNS name lookup and a traceroute back to the scanning host. Some scanners have software that alerts them when they have been tracerouted and they stop immediately, so LANcope watches closely for a while and logs data before launching the traceroute.

The important issue is to detect whenever a scanner finds a vulnerable host. LANcope is designed to recognize when a local host responds to a suspicious (High CI) host with more that a TCP Reset or an ICMP "No Listener," and will then alert the network manager immediately. The fact that alarms occur only when there is a potential for damage makes the system much more valuable than a system that alarms at every scan.

Service Locking

LANcope keeps a database of what Services each local host is allowed to offer (as a server), or access (as a client). If a Flow does not fit this Host Service Profile, the discrepancy is noted and reported. To do this it is necessary to determine that the Flow was a valid connection, with a proper handshake and data being exchanged, or whether it is an aborted connection (a potential probe).

This technique will detect a host that is in stage 3 (above), whether the compromising software was installed by an over-the-network exploit, or by a Trojan Horse program.

Most network managers do not have the human resources to keep track of all the computers on their network, much less the details or what client and server applications are being run. LANcope solves this problem by automatically building the Host Service Profiles while operating in several progressive modes:

Mode 1: Local hosts, and Host Service Profile points (client and server services) are detected and profiles are built up.

Mode 2. Service profiles continue to build up, but every day the new Out-of-Profile (OoP) points are reported on a Web page. At the end of the day the new points are added to the relevant Host Service Profile.

Mode 3. The profiles are locked. New points are not automatically added to the Host Service Profiles. The network manager can inspect the list of OoP services on the Web and manually add some to the Host Service Profile if they feel it is justified, or delete services from a Host Service Profile if they feel the service should not be allowed (e.g., a personal Web server with vacation photos).

Mode 4. Service Profile Lockdown. As soon as an OoP service is detected, an alarm is sent to the network manager. If desired, LANcope can send packets designed to disrupt OoP connections.

Some of the Trojan Horse programs seen recently set up a server on one of the 65,000 ports available (say 31337 on host Alice) and wait for a particular type of scanning packet to activate a response. When this happens LANcope will detect the Flow and Alice's OoP server on port 31337 will be reported, with an immediate alarm if the system is operating in mode 4.

A compromised machine will frequently start using an FTP client to download a "root kit" and set up an Internet Relay Chat client (or even an IRC server) to tell all his buddies about the new conquest. These activities will show up as OoP services.

Hopefully you can go for years without a hacker compromising one of your hosts. But what about the story in last Sunday's paper about how to download software and listen to your favorite background music, or your hometown radio station on your PC. Many office workers will do this without having a thought about tying up limited Internet connection capacity. Fifty Web radios will completely use up the capacity of a T1 connection. What about the mail clerk who starts downloading tunes via Napster? LANcope will again report these activities as OoP services.

Even if Service Profile Lockdown is not used, the worst offenders will show up on the list of High Traffic Hosts, and on the All Local Hosts list with the "Multimedia" column checked.

Since the wait for a hacker attack will hopefully be a long boring period, LANcope provides a good deal of Network performance data just to remind you that it's on the job. It also shows you the CI noise level so that when an attack does occur, you can see the CI is well above the normal noise level and the alarm should be taken seriously.